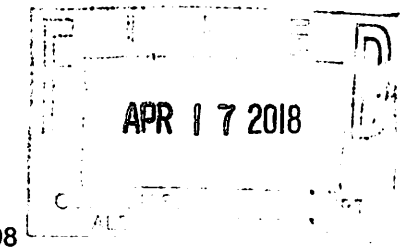
AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Samsung Model SM-J700T
S/N R58HB3NFVGL

Case No. 1:18-SW-198

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
Samsung Model SM-J700T, S/N R58HB3NFVGL, as further described in Attachment A (Property to be Searched).

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B (Property to be Seized).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 5332	Bulk Cash Smuggling; and
18 U.S.C. § 5316	Failure to File Currency Report.

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SAUSA Christopher Kaltsas/AUSA Dennis Fitzpatrick

William M. DeRose, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

/s/ JFA
John F. Anderson
United States Magistrate Judge
Judge's signature

Date: April 17, 2018

City and state: Alexandria, Virginia

Hon. John F. Anderson, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

The device to be searched includes a Samsung Cellular Phone, Model SM-J700T, Serial Number R58HB3NFVGL.

This warrant authorizes the forensic examination of the devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the devices described in Attachment A which constitute evidence, contraband, or instrumentalities of violations of 31 U.S.C. §§ 5332 including, but not limited to:

a. records regarding potential persons of interest and their related identifying and contact information;

b. records indicating purchased, or otherwise obtained, travel reservations and their related identifying and contact information;

c. text messages regarding the possession, production, sale, provision, and distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

d. records indicating companies or individuals involved in the request for, acquisition of, purchase, sale, manufacturing, storage, transport, receipt, concealment, or distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

e. emails regarding the possession, creation, production, sale, provision and distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

f. notes, photos, videos, or other electronically stored image or document regarding the possession, creation, production, sale, provision, and distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

g. contact lists or phonebooks contained on the devices or in applications accessible on the devices;

h. call lists contained on the devices or in applications accessible on the devices;

i. all calendar entries contained on the devices or in applications accessible on the devices;

j. reminders contained on the devices or in applications accessible on the devices;

k. a list of applications or software loaded onto the devices.

2. Evidence of who used, owned, or controlled the devices at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, phonebooks, photographs, videos, and correspondence.

3. Evidence of the presence or absence of software which would allow others to control the devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the attachment of the devices to other storage devices, phones, or similar containers for electronic evidence;

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the devices;

6. Evidence of the times the devices were used;

7. Passwords, encryption keys, and other access devices that may be necessary to access the devices;

8. Documentation and manuals that may be necessary to access the devices or to conduct a forensic examination of the devices;

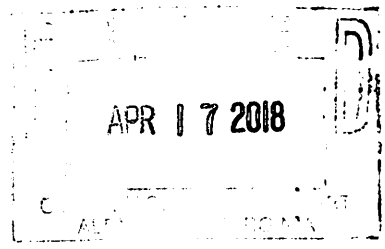
9. Records of or information about Internet Protocol addresses used by these devices;

10. Records of or information about the devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT IF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF AN ELECTRONIC DEVICES SEIZED AT DULLES INTERNATIONAL AIRPORT ON FEBRUARY 8, 2018: Samsung Cellular Phone, Model SM-J700T, Serial Number R58HB3NFVGL.	Case No. 1:18-SW-198

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

INTRODUCTION AND AGENT BACKGROUND

1. I, William DeRose, make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—namely, five electronic devices identified in Attachment A to this affidavit—that are currently in possession of law enforcement in Dulles, Virginia; and the extraction of electronically stored information from that property as described in Attachment B to this affidavit.

2. I am a Special Agent Criminal Investigator with United States Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"). ICE/HSI is a subordinate component of the Department of Homeland Security ("DHS"). I have been an ICE/HSI Special Agent since April 2009, and I am currently assigned to the Dulles International Airport Investigative Group at the HSI field office in Dulles, Virginia.

3. In my capacity as a Special Agent Criminal Investigator, I have had experience in criminal investigations involving human smuggling, human trafficking, financial crimes including bulk cash smuggling, narcotics smuggling, and identity/benefit fraud. I have been trained at the

Federal Law Enforcement Training Center in Brunswick, Georgia, where I have attended and graduated from the Criminal Investigator Training Program and the Immigration and Customs Special Agent Training Program. In my capacity as a Special Agent, my duties include investigating violations of the nation's immigration, nationality, and customs laws.

4. The facts and information contained in this affidavit are based upon my training and experience, participation in investigations, personal knowledge, and observations during the course of this investigation, as well as the observations of other agents and officers involved in this investigation. All observations not personally made by me were relayed to me by individuals who made them or are based on my review of records, documents and other physical evidence obtained during the course of this investigation. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. For the reasons set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 31, United States Code, Sections 5316 and 5332, namely: knowingly concealing more than $10,000 in currency or other monetary instruments without declaring those assets, when declaration of such assets is necessary, on the person of such individual or in any conveyance, article of luggage, merchandise, or other container, and transporting or transferring or attempting to transfer such currency or monetary instruments from a place within the United States to a place outside the United States, or from a place outside the United States to a place within the United States.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. I seek a warrant to search a Samsung Cellular Phone, Model SM-J700T, Serial Number R58HB3NFVGL. The item referenced herein will be identified as "the device," which

were found in Jerry Quincy Tetteh-Quartey's ("TETTEH-QUARTEY's") possession while he was attempting to depart the United Stations aboard an international flight with over $80,000 in unreported US currency, which far exceeds the reporting requirement of $10,000 pursuant to 18 U.S.C. §§ 5316, 5332. The device is currently located at 44965 Aviation Drive, Suite 112, Dulles, VA 20166.

7. The applied-for warrant would authorize the forensic examination of the device described in Exhibit A for the purpose of identifying electronically stored data particularly described in Attachment B.

RELVEVANT STATUTES

8. Title 31, United States Code, Section 5316, provides that:

> a person ... shall file a report . . . when the person . . . knowingly transports, is about to transport, or has transported, monetary instruments of more than $10,000 at one time from a place in the United States to or through a places outside the United States; or to a place in the United States from or through a place outside the United States; or receives monetary instruments of more than $10,000 at one time transported into the United States from or through a place outside the United States.

9. Title 31, United States Code, Section 5332 provides that:

> [w]hoever, with the intent to evade a currency reporting requirement under Section 5316, knowingly conceals more than $10,000 in currency or other monetary instruments on the person of such individual or in any conveyance, articles of luggage, merchandise, or other container, and transports or transfers or attempts to transfer such currency or monetary instruments from a place within the United States to a place outside the United States, . . . shall be guilty of a currency smuggling offense.

PROBABLE CAUSE

10. On February 8, 2018, TETTEH-QUARTEY attempted to depart the United States from the Washington Dulles International Airport (IAD), in Dulles, Virginia, aboard South African

Airways flight SA 210 from IAD to Accra, Ghana at approximately 4:55 p.m. Uniformed Officers of the United States Customs and Border Protection ("CBP" or "USCBP") were conducting an outbound currency operation on SA flight 210 when they encountered TETTEH-QUARTEY, as he attempted to board flight SA 210 and depart the United States. Upon encountering TETTEH-QUARTEY at the departure gate, CBP Officer Kane provided TETTEH-QUARTEY a currency reporting form and verbally explained to TETTEH-QUARTEY the currency reporting requirements for anyone departing or arriving into the United States. TETTEH-QUARTEY provided Officer Kane a valid permanent resident card bearing identification number A059106003, and a Ghanaian passport bearing identification number H2672878, which verified TETTEH-QUARTEY's identity.

11. Officer Kane then proceeded to question TETTEH-QUARTEY as to the total amount of currency on his person and in his luggage. TETTEH-QUARTEY stated that he was traveling with $7,800.00 in currency. Officer Kane advised TETTAH-QUARTEY that he could carry any amount of currency, but if the amount was more than $10,000, he would have to fill out a Currency and Other Monetary Instruments Report ("CMIR" or FINCEN Form 105). TETTEH-QUAREY verified he understood these instructions and wrote the amount with which he was traveling on the backside of a CBP form 503 as $7,800. TETTEH-QUARTEY signed the form and provided it to Officer Kane. Officer Kane then moved TETTEH-QUARTEY to a private area, to verify the amount of currency TETTEH-QUARTEY was transporting. TETTEH-QUARTEY informed Officer Kane some of the currency he was traveling with was his and some belonged to his aunt.

12. Officer Kane then began to search TETTEH-QUARTEY's carry-on luggage. During the inspection of TETTEH-QUARTEY's carry-on backpack, Officer Kane discovered two

brown and one black wallets. Each wallet contained different amounts of U.S. currency including, respectively, $5,500; $4,700; and $5,706. The amount of currency in these wallets totaled $15,906. After this discovery, Officer Kane asked TETTEH-QUARTEY why he underreported how much currency he was traveling with after acknowledging that he understood the reporting requirements. TETTEH-QUARTEY responded that "someone" told him that if anyone asked him how much money he was carrying, to deny he had any money. TETTEH-QUARTEY refused to identify this person. Officer Kane subsequently informed TETTEH-QUARTEY that he would search the remainder of his luggage, to which TETTEH-QUARTEY replied, "Now I'm really in trouble."

13. A search of TETTEH-QUARTEY's second carryon bag revealed a backpack. Inside of this backpack, Officer Kane discovered a zipped black portfolio containing $67,187 in United States currency. After TETTEH-QUARTEY's initial declaration of only having $7,800 in currency, a total amount of $83,093 U.S. dollars was discovered on his person as he attempted to board SA flight 210.

14. Based upon this discovery and further questioning, TETTEH-QUARTEY informed Officer Kane that approximately $20,000 belonged to him and the remaining amount belonged to his aunt. TETTEH-QUARTEY claimed he was carrying the currency to help fund a project in Ghana. Officer Kane discovered what appeared to be architectural drawings contained within TETTEH-QUARTEY's carryon bag with his name listed as the client. Officer Kane asked TETTEH-QUARTEY if he was being paid by anyone to transport the US currency out of the country, to which he replied "no." Other USCBP officers then contacted a SA Airways representative, informing them of the situation concerning traveler TETTEH-QUARTEY and to have his checked luggage offloaded and transported to the IAD main terminal. In addition to the unreported U.S. currency, TETTEH-QUARTEY also had in his possession four cellular phones

and one Apple iPad. TETTEH-QUARTEY was transported to the USCBP secondary inspection site located at IAD for further inspection of TETTEH-QUARTEY's checked luggage.

15. Further inspection of TETTEH-QUARTEY's checked luggage discovered ten (new in box) iPhone Xs, six (new in box) Dell Inspiron laptop computers, one (new in box) HP Pavilion laptop computer, and one (new in box) MacBook Air laptop computer. TETTEH-QUARTEY informed CBP Officer Kane that he was planning to sell these items in Ghana. Further inspection of TETTEH-QUARTERY's person also revealed that he held several PayPal prepaid cards on his person, some still affixed with an "Activate Online" sticker. Additionally, several credit cards from various banking institutions were also in TETTEH-QUARTEY's possession.

16. At approximately 5:45 pm, HSI Special Agents (SAs) Michael Stempinski and Alan Poorman arrived at the IAD CBP secondary inspection site upon receiving information concerning the outbound currency inspection of TETTEH-QUARTEY. After conducting a discussion with CBP officers concerning their discoveries related to TETTEH-QUARTEY, at approximately 7:40 pm, SA Stempinski and SA Poorman attempted to interview TETTEH-QUARTEY. They introduced themselves to TETTEH-QUARTEY and explained the purpose of the interview. Prior to asking any questions, the agents provided TETTEH-QUARTEY a "Statement of Rights" form. TETTEH-QUARTEY informed the agents that he understood his rights as explained by this form and that he would not answer any questions at that time. Additionally, TETTEH-QUARTEY refused to provide any assistance in unlocking the devices found on his person, to assistance with any inspection of the devices. The unreported U.S. currency and discovered devices were seized for further investigation pending obtaining a judicially authorized search warrant.

17. In relation to the five devices, an Apple iPhone, Model A1532, was found on TETTEH-QUARTEY's person with the wallets containing $15,906 of unreported U.S. currency. This phone received several missed calls from various phone numbers and contacts, including: (1) phone number (301) 683-5940; (2) a contact identified as "Phloot mtn;" (3) phone number (301) 952-6000; and (4) a contact identified as "Danny Botchway." Throughout his outbound inspection, TETTEH-QUARTEY made repeated requests to USCBP Officers to use this device.

18. Based on TETTEH-QUARTEY's repeated refusals to reveal the identities of those with whom he attempted to contact, it is my belief that TETTEH-QUARTEY attempted to stop law enforcement from identifying contacts that may have been involved in the instant criminal activity. In my previous experience, I have seen that cellular phones and iPad laptops, such as the device described in Exhibit A, are often used to carry out and/or facilitate bulk cash smuggling and the transportation of concealed monetary instruments in violation of 31 U.S.C § 5332 by facilitating communications between members of a conspiracy to commit said conduct. Moreover, in my previous experience, I have learned that Ghana is a source country for illegal activity facilitated by United States currency. One such example is money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957; in my experience, I have seen bulk cash smuggling used to engage in such activity. Moreover, in my previous experience, I have seen that cellular phones and iPad laptops, such as the device described in Exhibit A, are often used to carry out and/or facilitate money laundering activities and the transportation and spending of proceeds of specified unlawful activities.

19. I submit that there is probable cause to believe that TETTEH-QUARTEY utilized and attempted to utilize the device described in Attachment A to communicate with several contacts during the time of his planned departure from IAD, while in the possession of over

$80,000 unreported U.S. currency. This belief is based on his repeated requests to use the device while detained and his refusal to provide information pertaining to the device during his interview with law enforcement. I also base this belief on the blatant lies TETTEH-QUARTEY told USCBP officers prior to the search of his carry-on luggage and his refusal to identify any of the people with whom he was communicating. I accordingly believe, based on these circumstances, that the device contain evidence, and are themselves instrumentalities of criminal conduct committed by TETTEH-QUARTEY in furtherance of his intent to provide false statements to conceal his possession of large amounts of unreported U.S. currency while attempting to depart the United States, in violation of 31 U.S.C. § 5332. I also believe that a search of the device may elicit evidence of TETTEH-QUARTEY's involvement in other financial crimes.

20. Based on my training and experience, I know that violators of 31 U.S.C. § 5332 frequently use cell phones and iPad laptops, such as the device described in Exhibit A, to communicate information relevant to conspiracies related to bulk cash smuggling or the smuggling of monetary instruments into or out of the United States. Such communications may take the form of text messages, emails, and other forms of electronic communication which, based on my training and experience, I know can remain on phones and SIM cards for years.

21. Based on my training and experience, I also know that conspirators often retain pictures on their cell phones and iPad laptops, such as the device described in Exhibit A, which link them to co-conspirators and document acts in furtherance of conspiracies to facilitate the importation and distribution of unreported currency into and throughout the United States.

22. Based on my training and experience, I also know that cell phones and iPad laptops identified as the device described in Exhibit A, often contain information, including GPS information, showing the owner's possible location at various times.

23. The device is currently in the lawful possession of the DHS/HSI. It came into the DHS/HSI's possession during the outbound customs inspection of TETTEH-QUARTEY as an international passenger attempting to depart from the United States on February 8, 2018.

24. The device is currently in storage at 44965 Aviation Drive, Suite 112, Dulles, Virginia, 20166. I know that the device has been in the continuous possession of law enforcement and has been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as it was when it first came into the possession of the DHS/HSI.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading

information from the Internet. Wireless telephones may also include global positioning system technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. A portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved

in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address

so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. SIM Card: A SIM Card is a small card that contains cellular network subscriber's account information which allows the device to authenticate to the network on which it is connected. SIM Cards may store limited amounts of recoverable data such as phone numbers, text messages, location information to include last connected tower, phone book, and subscriber information. Moving a SIM Card from one phone to another allows a subscriber to switch cell phones without having to contact their network carrier.

i. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at https://support.apple.com, https://www.samsung.com, and https://support.sprint.com, I know that the devices have capabilities which allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that

reveals or suggests who possessed or used the device along with evidence tied to importing prohibited items via phone contacts with co-conspirators, text messages with co-conspirators, photos of co-conspirators and locations where the exchange of prohibited items is occurring, GPS coordinates detailing where various co-conspirators are located, IP logs indicating where the user of the phone was located when accessing the internet, among other things.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices and related SIM Cards because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on storage media that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, which might expose parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the

physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

30. I submit that this affidavit supports probable cause for a search warrant authorizing examination of the device described in Attachment A to seek that described in Attachment B.

REQUEST FOR SEALING

31. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation that is neither public nor known to all of the targets of the investigation. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

William M. DeRose
Special Agent
Homeland Security Investigations
U.S. Department of Homeland Security

Subscribed and sworn to before me
on April 17, 2018:

/s/
John F. Anderson
United States Magistrate Judge

The Hon. John F. Anderson
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The device to be searched includes a Samsung Cellular Phone, Model SM-J700T, Serial Number R58HB3NFVGL.

This warrant authorizes the forensic examination of the devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the devices described in Attachment A which constitute evidence, contraband, or instrumentalities of violations of 31 U.S.C. §§ 5332 including, but not limited to:

a. records regarding potential persons of interest and their related identifying and contact information;

b. records indicating purchased, or otherwise obtained, travel reservations and their related identifying and contact information;

c. text messages regarding the possession, production, sale, provision, and distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

d. records indicating companies or individuals involved in the request for, acquisition of, purchase, sale, manufacturing, storage, transport, receipt, concealment, or distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

e. emails regarding the possession, creation, production, sale, provision and distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

f. notes, photos, videos, or other electronically stored image or document regarding the possession, creation, production, sale, provision, and distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

g. contact lists or phonebooks contained on the devices or in applications accessible on the devices;

h. call lists contained on the devices or in applications accessible on the devices;

i. all calendar entries contained on the devices or in applications accessible on the devices;

j. reminders contained on the devices or in applications accessible on the devices;

k. a list of applications or software loaded onto the devices.

2. Evidence of who used, owned, or controlled the devices at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, phonebooks, photographs, videos, and correspondence.

3. Evidence of the presence or absence of software which would allow others to control the devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the attachment of the devices to other storage devices, phones, or similar containers for electronic evidence;

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the devices;

6. Evidence of the times the devices were used;

7. Passwords, encryption keys, and other access devices that may be necessary to access the devices;

8. Documentation and manuals that may be necessary to access the devices or to conduct a forensic examination of the devices;

9. Records of or information about Internet Protocol addresses used by these devices;

10. Records of or information about the devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.